

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the
Northern District of New York

UNITED STATES OF AMERICA)

v.)

Case No. 3:22-MJ- 333 (ATB)

PHILIP KOESTER,)

Defendant)

U.S. DISTRICT COURT – N.D. OF N.Y.

FILED

Jul 01 - 2022

John M. Domurad, Clerk

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date of January 13, 2016 in the county of Broome in the Northern District of New York the defendant violated:

*Code Section*Title 18, United States Code, Section
2252A(a)(5)*Offense Description*

Knowingly Possessing Child Pornography

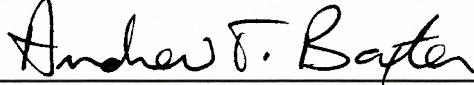
This criminal complaint is based on these facts:
See attached affidavit☒ Continued on the attached sheet.*Complainant's signature*

Jenelle Corrine Bringuel, Special Agent

Printed name and title

Attested to by the affiant in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.

Date: 7/1/2022

*Judge's signature*

City and State: Syracuse, New York

Hon. Andrew T. Baxter, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

I, Jenelle Bringuel, having been first duly sworn, do hereby depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent of the FBI since June 2012 and am currently assigned to the Albany Division, Binghamton Resident Agency. I am specifically assigned to the Mid-State Child Exploitation Task Force (MSCETF), which targets individuals involved in the on-line sexual exploitation of children. As part of my duties, I investigate crimes involving the sexual exploitation of minors, including sex trafficking of minors and various criminal offenses related to the production, distribution, receipt, and possession of child pornography. I received training on the proper investigative techniques for these violations, including the use of surveillance techniques, undercover activities, and the application and execution of arrest and search warrants. I have conducted and assisted in several child exploitation investigations, and have executed search warrants that have led to seizures of child pornography and undercover operations to identify and locate individuals who seek to engage in sexual activity with minors.

2. I am an investigative or law enforcement officer of the United States within the meaning of Title 18 United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516(1). As an FBI Special Agent, I am authorized to seek and execute federal arrest warrants for Title 18 criminal offenses, including offenses related to the sexual exploitation of minors.

3. I make this affidavit in support of a criminal complaint charging PHILIP KOESTER

with knowingly possessing child pornography, in violation of Title 18, United States Code, Section 2252A(a)(5).

4. The statements contained in this affidavit are based upon my investigation, information provided by other law enforcement officers, and on my experience and training as a Special Agent of the FBI. As this affidavit is being submitted for the limited purpose of securing a criminal complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that KOESTER has violated Title 18, United States Code, Section 2252A(a)(5).

OVERVIEW

5. PHILIP KOESTER was part of an online community of individuals who regularly sent and received child pornography via a website that operated on an anonymous online network. The website is described below and referred to herein as “Website A.”¹ After receiving child pornography online KOESTER saved it to electronic digital devices he owned. A federal search warrant conducted on KOESTER’s residence on January 13, 2016, revealed that KOESTER knowingly possessed 1318 image and 21 video files depicting minors engaged in sexually explicit conduct on a Western Digital hard drive model WD6401AALS, serial number WMATV7402865 manufactured in Malaysia/Thailand.

THE NETWORK²

¹ The actual name of “Website A” is known to law enforcement. Disclosure of the name of the site would potentially alert its members that law enforcement action is being taken against the site and its users, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the website will be identified as “Website A.”

² The actual name of the Network is known to law enforcement. The network remains active and disclosure of the name of the network would potentially alert its members to the fact that law

6. “Website A” operated on a network (“the Network”) available to Internet users who were aware of its existence. The Network is designed specifically to facilitate anonymous communication over the Internet. In order to access the Network, a user must install computer software that is publicly available, either by downloading software to the user’s existing web browser, downloading free software available from the Network’s administrators, or downloading a publicly-available third-party application.³ Using the Network prevents someone attempting to monitor an Internet connection from learning what websites a user visits and prevents the websites the user visits from learning the user’s physical location. Because of the particular way the Network routes communication through other computers, traditional IP identification techniques used by law enforcement agencies are not viable.

7. Websites that are accessible only to users within the Network can be set up within the Network and “Website A” was one such website. Accordingly, “Website A” could not generally be accessed through the traditional Internet.⁴ Only a user who had installed the appropriate software on the user’s computer could access “Website A.” Even after connecting to the Network, however, a user had to know the exact web address of “Website A” in order to access it. Websites on the Network

enforcement action is being taken against the network, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the network will be identified as “the Network.”

³ Users may also access the Network through so-called “gateways” on the open Internet, however, use of those gateways does not provide users with the full anonymizing benefits of the Network.

⁴ Due to a misconfiguration, prior to February 20, 2015, “Website A” was occasionally accessible through the traditional Internet. In order to access “Website A” in that manner, however, a user would have had to know the exact IP address of the computer server that hosted “Website A”, information which was not publicly available. As of on or about February 20, 2015, “Website A” was no longer accessible through the traditional Internet.

are not indexed in the same way as websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user could not simply perform a Google search for the name of “Website A,” obtain the web address for “Website A,” and click on a link to navigate to “Website A.” Rather, a user had to have obtained the web address for “Website A” directly from another source, such as other users of “Website A,” or from online postings describing both the sort of content available on “Website A” and its location. Therefore, accessing “Website A” required numerous affirmative steps by the user, making it extremely unlikely any user could have simply stumbled upon “Website A” without first understanding its content and knowing that its primary purpose was to advertise and distribute child pornography.

8. The Network’s software protects users’ privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user’s actual IP address which could otherwise be used to identify a user.

9. The Network also makes it possible for users to hide their locations while offering various kinds of services, such as web publishing, forum/website hosting, or an instant messaging server. Within the Network itself, entire websites can be set up which operate the same as regular public websites with one critical exception: the IP address for the web server is hidden and instead is replaced with a Network-based web address. A user can only reach such websites if the user is using the Network client and operating in the Network. Because neither a user nor law enforcement can identify the actual IP address of the web server, it is not possible to determine through traditional, public lookups where the computer that hosts the website is located. Accordingly, it is not possible to obtain data detailing the activities of the users from the website server through public lookups.

DESCRIPTION OF “WEBSITE A” AND ITS CONTENT

10. “Website A” was a child pornography bulletin board and website dedicated to the

advertisement and distribution of child pornography and the discussion of matters pertaining to the sexual abuse of children including the safety and security of individuals who seek to sexually exploit children online. On or about February 20, 2015, the computer server hosting “Website A” was seized from a web-hosting facility in Lenoir, North Carolina. The website operated in Newington, Virginia from February 20, 2015 until March 4, 2015, at which time “Website A” ceased to operate. Between February 20, 2015, and March 4, 2015, law enforcement agents acting, pursuant to an order of the United States District Court for the Eastern District of Virginia, monitored electronic communications of users of “Website A.” Before, during, and after its seizure by law enforcement, law enforcement agents viewed, examined and documented the contents of “Website A,” which are described below.

11. According to statistics posted on the site, “Website A” contained a total of 117,773 posts, 10,622 total topics, and 214,898 total members as of March 4, 2015. The website appeared to have been operating since approximately August 2014, which is when the first post was made on the message board. Between September of 2014 and February 19, 2015, on the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent girls with their legs spread apart, along with the text underneath stating, “No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out.”⁵ Based on my training and experience, I know that: “no cross-board reposts” refers to a prohibition against material that is posted on other websites from being “re-posted” to “Website A;” and “.7z” refers to a preferred method of compressing large files or sets of files for distribution. Two data-entry fields with a corresponding “Login” button were located to the right of the site name. Located below the aforementioned items

⁵ On February 19, 2015, the site administrator replaced those two images with a single image, located to the left of the site name, depicting a prepubescent female, wearing a short dress and black stockings, posed sitting reclined on a chair with her legs crossed, in a sexually suggestive manner, and the text “No cross-board reposts, .7z preferred, Encrypt filenames, Include preview,” to the right of the image.

was the message, "Warning! Only registered members are allowed to access the section. Please login below or 'register an account' [(a hyperlink to the registration page)] with "[Website A]." Below this message was the "Login" section, consisting of four data-entry fields with the corresponding text, "Username, Password, Minutes to stay logged in, and Always stay logged in."

12. Upon accessing the "register an account" hyperlink, there was a message that informed users that the forum required new users to enter an e-mail address that looks to be valid. However, the message instructed members not to enter a real e-mail address. The message further stated that once a user registered (by selecting a user name and password), the user would be able to fill out a detailed profile. The message went on to warn the user, "[F]or your security you should not post information here that can be used to identify you." The message further detailed specific rules for the forum and provided other recommendations regarding how to hide the user's identity for the user's own security.

13. After accepting the above terms, registration to the message board then required a potential user to enter a username, password, and e-mail account; although, a valid e-mail address and account was not required as described above.

14. After successfully registering and logging into the site, the user could access any number of sections, forums, and sub-forums. Some of the sections, forums, and sub-forums available to users included: (a) How to; (b) General Discussion; (c) [Website A] information and rules; and (d) Security & Technology discussion. Additional sections, forums, and sub-forums included (a) Jailbait – Boy; (b) Jailbait – Girl; (c) Preteen – Boy; (d) Preteen – Girl; (e) Pre-teen Videos – Girl HC; (f) Pre-teen Videos – Boys HC; (g) Toddlers; and (h) Kinky Fetish – Scat. Based on my training and experience, your affiant knows that "jailbait" refers to underage but post-pubescent minors; the abbreviation "HC" means hardcore (i.e., depictions of penetrative sexually explicit conduct); and

“scat” refers to the use of feces in various sexual acts, watching someone defecating, or simply seeing the feces. An additional section and forum was also listed in which members could exchange usernames on a Network-based instant messaging service your affiant knows, based upon my training and experience, to be commonly used by subjects engaged in the online sexual exploitation of children.

15. A review of the various topics within the above forums revealed each topic contained a title, the author, the number of replies, the number of views, and the last post. The “last post” section of a particular topic included the date and time of the most recent posting to that thread as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any corresponding replies to the original post included in the post thread below it. Typical posts had text, images, thumbnail-sized previews of images, compressed files (such as Roshal Archive files, commonly referred to as “.rar” files, which are used to store and distribute multiple files within a single file), links to external web sites, or various replies to previous posts.

16. A review of the various topics within the “[Website A] information and rules,” “How to,” “General Discussion,” and “Security & Technology discussion” forums revealed that the majority of these topics contained general information in regards to the web site, instructions and rules for users regarding how to post, and welcome messages between various users.

17. A review of the topics within the remaining forums revealed the majority contained discussions about child pornography, and numerous images that depicted child pornography and child erotica. Examples of some of these posts are as follows:

- a. On February 3, 2015, a user posted a topic entitled “Buratino-06” in the forum “Pre-teen – Videos - Girls HC” that contained numerous images depicting child pornography of a prepubescent or early pubescent girl. One of these

- images depicted the girl being orally penetrated by the penis of a naked male;
- b. On January 30, 2015, a user posted a topic entitled “Sammy” in the forum “Pre-teen – Photos – Girls” that contained hundreds of images depicting child pornography of a prepubescent girl. One of these images depicted the female being orally penetrated by the penis of a male; and
 - c. On September 16, 2014, a user posted a topic entitled “9yo Niece - Horse.mpg” in the “Pre-teen Videos - Girls HC” forum that contained four images depicting child pornography of a prepubescent girl and a hyperlink to an external website that contained a video file depicting what appeared to be the same prepubescent girl. Among other things, the video depicted the prepubescent female, who was naked from the waist down with her vagina and anus exposed, lying or sitting on top of a naked adult male, whose penis was penetrating her anus.

18. A list of members, which was accessible after registering for an account, revealed that approximately 100 users made at least 100 posts to one or more of the forums. Approximately 31 of these users made at least 300 posts. In total, “Website A” contained thousands of postings and messages containing child pornography images. Those images included depictions of nude prepubescent minors exposing their genitals or engaged in sexually explicit conduct with adults or other children.

19. “Website A” also included a feature referred to as “[Website A] Image Hosting.” This feature of “Website A” allowed users to upload links to images of child pornography that are accessible to all registered users of “Website A.” On February 12, 2015, an FBI Special Agent accessed a post on “Website A” titled “Giselita” which was created by a particular “Website A” user. The post contained links to images stored on “[Website A] Image Hosting.” The images depicted a

prepubescent girl in various stages of undress. Some images were focused on the nude genitals of a prepubescent girl. Some images depicted an adult male's penis partially penetrating the vagina of a prepubescent girl.

20. Text sections of “Website A” provided forums for discussion of methods and tactics to use to perpetrate child sexual abuse and exploitation:

- a. On January 8, 2015, a user posted a topic entitled "should i proceed?" in the forum “Stories - Non-Fiction” that contained a detailed accounting of an alleged encounter between the user and a 5 year old girl. The user wrote “...it felt amazing feeling her hand touch my dick even if it was through blankets and my pajama bottoms...” The user ended his post with the question, “should I try to proceed?” and further stated that the girl “seemed really interested and was smiling a lot when she felt my cock.” A different user replied to the post and stated, “...let her see the bulge or even let her feel you up...you don't know how she might react, at this stage it has to be very playful...”

COURT AUTHORIZED USE OF NETWORK INVESTIGATIVE TECHNIQUE

21. Websites generally have Internet Protocol (“IP”) address logs that can be used to locate and identify the site’s users. In such cases, after the seizure of a website whose users were engaging in unlawful activity, law enforcement could review those logs in order to determine the IP addresses used by users of “Website A” to access the site. A publicly available lookup could then be performed to determine what Internet Service Provider (“ISP”) owned the target IP address. A subpoena could then be sent to the ISP to determine the user to which the IP address was assigned at a given date and time.

22. However, because of the Network software utilized by “Website A,” any such logs of

user activity would contain only the IP addresses of the last computer through which the communications of “Website A” users were routed before the communications reached their destinations. The last computer is not the actual user who sent the communication or request for information, and it is not possible to trace such communications back through the Network to that actual user. Such IP address logs, therefore, could not be used to locate and identify users of “Website A.”

23. Accordingly, on February 20, 2015, the same date “Website A” was seized, the United States District Court for the Eastern District of Virginia authorized a search warrant to allow law enforcement agents to deploy a Network Investigative Technique (“NIT”) on “Website A” in an attempt to identify the actual IP addresses and other identifying information of computers used to access “Website A.” Pursuant to that authorization, between February 20, 2015 and approximately, March 4, 2015, each time any user or administrator logged into “Website A” by entering a username and password, the FBI was authorized to deploy the NIT which would send one or more communications to the user’s computer. Those communications were designed to cause the receiving computer to deliver to a computer known to or controlled by the government, data that would help identify the specific computer, its location, other information about the computer, and the user of the computer accessing “Website A.” That data included: the computer’s actual IP address, and the date and time that the NIT determined what that IP address was; a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of other computers; the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86); information about whether the NIT had already been delivered to the computer; the computer’s Host Name; the computer’s active operating system username; and the computer’s MAC address.

USER “REIDICK” ON “WEBSITE A”

24. According to data obtained from logs on “Website A,” monitoring by law enforcement agencies involved in this investigation, and the deployment of the NIT, a user with the user name, “reidick”, engaged in the below listed activity on “Website A.”

25. The profile page of user “reidick” indicated this user originally registered an account on “Website A” on October 11, 2014. Profile information on “Website A” may include contact information and other information that is supplied by the individual user. It also contains information about that particular user’s participation on the website including statistical information about the user’s posts to the website and a categorization of those particular posts. According to the user “reidick’s” profile, this user was a “Newbie Member” of “Website A.” Furthermore, according to the Statistics section of this user’s profile, the user “reidick” had been actively logged into the “Website A” for a total of 97 hours and 27 minutes between the dates of October 11, 2014 and February 27, 2015.

26. According to the statistics on user “reidick’s” profile page, between October 11, 2014, and February 27, 2015, this user made a total of approximately 12 postings to “Website A.” However, according to data obtained from logs on “Website A,” this user actually made a total of 15 posts. This difference in accounting was likely due to certain posts made by users that had been inadvertently removed from the website at some point by the administrator during maintenance of the website. However, these posts were still maintained in backup logs of “Website A” and show that the user “reidick” posted 15 times. Examples and descriptions of some of “reidick’s” posts are as follows:

- a. On January 22, 2015, the user “reidick” made a post in response to posts made

by other users to a forum entitled “Short vids [First Post].” In his post, the user “reidick” posted three hyperlinks to external websites and the text, “oh shit....thank you so much. I’ve looking for one of those for so long. There is actually more of one of those girls. Looks like she squirts in the 2nd video. I want that one so fucking bad. Girl is perfect.” Each of the three hyperlinks posted by the user “reidick” contained an image depicting a prepubescent or early pubescent female. One of these images depicted an early pubescent female with her legs spread apart, exposing her vagina and vaginal area, which was being penetrated by a dark-colored cylindrical object. The hyperlinks posted by the other users in this forum also contained child pornography and child erotica material depicting early pubescent females.

- b. On October 7, 2014, another user made a post that included a hyperlink to a preview image, also known as a contact sheet, as well as a hyperlink to an external website containing the full file and a password to open the file. The contact sheet contained 30 smaller images, the majority of which contained child pornography and child erotica depicting a prepubescent female; including images depicting the vaginal penetration of this female. The hyperlink to the full file was not accessible. In response to this post, on December 12, 2014, the user “reidick” made a post stating, “Pretty weird... I know a girl IRL named Abbie that looks just like her. She’s like 30... but they could be sisters.”

IP ADDRESS AND IDENTIFICATION OF USER “REIDICK” ON “WEBSITE A”

27. According to data obtained from logs on “Website A,” monitoring by law enforcement agencies involved in this investigation, and the deployment of a NIT, the user “reidick” engaged in

the following activity on February 26, 2015 on “Website A” from IP address, 67.246.151.19. On February 26, 2015, the user “reidick” with IP address, 67.246.151.19, accessed the post entitled “[OFFER] Taking ‘Girls Cams’ Requests” in the “Webcams – Girls” forum. This post contained the text, along with additional text, “As many of you know, there are 9 sites for girls cams, each with 100 cams per page. (Another website known to law enforcement agencies to be engaged in the online sexual exploitation of children) started doing requests but there were too many request from lurkers so now there are 3 rules from me. 1. Only requests from users with at least 15 thanks will be fulfilled. 2. In a reply, post the link to the specific vid you want 3. No requesting password information for the girls cams sites. For those who don’t know the girls cam site links, there are here:” Nine hyperlinks to other websites on the Network were then listed. These websites are known to law enforcement to contain child pornography and child erotica depicting prepubescent and early pubescent females including those depicting prepubescent females with their legs spread apart, exposing their vaginas, and those depicting a prepubescent female being orally penetrated by a male’s penis.

28. Using publicly available websites, FBI Special Agents were able to determine the IP address, 67.246.151.19, was operated by the “ISP” Time Warner Cable.

29. In March 2015, an FBI administrative subpoena was served on Time Warner Cable requesting subscriber information regarding the user who was assigned to the IP address, 67.246.151.19, on February 26, 2015. According to the information received from Time Warner Cable pursuant to the subpoena, PHILIP KOESTER was receiving Internet service at 33 Jane Lacey Drive, Apt. N, Endicott, New York 13760 on February 26, 2015, with an activation date of May 03, 2013.

30. On October 5, 2015, an FBI administrative subpoena was served on the New York State Electric and Gas Corporation (NYSEG) requesting information regarding services being

provided at 33 Jane Lacey Drive, Apt. N, Endicott, New York 13760. On October 6, 2015, NYSEG provided customer information indicating PHILIP KOESTER was receiving and paying for electric and gas services at 33 Jane Lacey Drive, Apt. N, Endicott, New York 13760.

31. On October 5, 2015, a check of open source information on the Internet regarding PHILIP KOESTER revealed a LinkedIn profile for “Phil Koester, Endicott, New York.” According to this profile, “Phil Koester” has been employed at Fiber Tech/Engineer at Time Warner Cable Business Class since June 2012 and was previously employed at MCM Solutions, LLC as an Installation Tech from March 2009 through May 2012. On October 5, 2015 while conducting physical surveillance at 33 Jane Lacey Drive, Apt. N, Endicott, New York 13760, law enforcement observed a Time Warner Cable Business Class Ford F150 utility pickup truck and a green colored 2004 Ford Escape with the New York State license plate, GBS8527, registered to a PHILIP KOESTER, date of birth XX/XX/1986. These vehicles were parked in close proximity of each other and directly outside the northwestern corner of Building 33 near the communal entrance to Apartments M, N, O, and P.

32. On December 28, 2015, a search of the New York State Department of Motor Vehicles indicated PHILIP KOESTER, date of birth XX/XX/1986, was residing at 33 Jane Lacey Drive, Apt. N, Endicott, New York 13760. Moreover, PHILIP KOESTER maintained a valid vehicle registration on a green colored 2004 Ford Escape with the New York State license plate, GBS8527.

33. On December 28, 2015, an additional FBI administrative subpoena was served on Time Warner Cable requesting information regarding the user who was assigned the IP address, 67.246.151.19, on December 27, 2015 at 12:00 p.m. According to the information received from Time Warner Cable on December 29, 2015, PHILIP KOESTER was still receiving the same type of Internet services via that IP Address at 33 Jane Lacey Drive, Apt. N, Endicott, New York 13760 as of that date.

34. On January 13, 2016, a federal search warrant (3:16-MJ-7 (ATB)) was executed at KOESTER's residence in Endicott, New York. As a result of the execution of this search warrant, multiple digital evidence items were seized and searched. A forensic examination of these items was conducted by the FBI's Digital Analysis and Research Center. Many of the items were found to be encrypted. Non-encrypted items and items that were able to be decrypted were processed for logical and deleted files and the deleted files were recovered where possible. Thousands of image and video files were located that depict either the sexual abuse and/or exploitation of children. A text file named "logins.txt" was recovered from a Lian Li desktop computer (seized from Koester's residence) that contains a list of login IDs and passwords, many of which are related to Phil Koester. One such entry from the text file lists the password "niggerfaggot". Variants of that password were also observed. This password was known by law enforcement to be used by the user "reidick" in order to access Website A.

35. Artifacts related to the use of an un-encrypted Linux based operating system running a virtual machine were also found on the aforementioned Lian Li desktop computer owned by KOESTER, to include:

- The user, "Helix" visited online child exploitation/abuse predicated chat rooms.
- Thumbnail files generated by the operating system of the device were identified and appear to depict the sexual abuse and/or exploitation of children. These thumbnail files contain embedded metadata that includes the original file name and path to the original full size image or video. Most of the file paths for these thumbnails show that the original files were stored on encrypted drives.
- Tens of thousands of Freenet and Frost bulletin board posts were identified to include postings by the user 'wat' which appears to be linked to PHILIP KOESTER.

Most of the posts appear to be related to the exploitation and abuse of children.

- A recently accessed files list was identified that lists the times and dates that recent files had been accessed, the file names, the path to the file, and the application that opened the files. Many of the file names were found to be indicative of child abuse material.
- TOR activity by user “reidick” was found.
- Numerous folders were identified on the Lian Li desktop computer that contained images and videos of various females separated and grouped in folders by name. One of these series folders named “Velma” contained information indicating that the female shown in the child abuse material depictions was under the age of 18.
- Recovered artifacts showing that the home built desktop computer accessed the internet via public IP address 67.246.151.19 in February of 2015.

36. On the aforementioned home built desktop computer, 1318 image and 21 video files depicting minors engaged in sexually explicit conduct were located on the Western Digital hard drive model WD6401AALS, serial number WMATV7402865 manufactured outside the state of New York. Ninety-eight (98) of these files depicted infants/toddlers. Two of these files are described below and are available for the court’s review upon request:

- File: MSA Fivestar personal gas alarm teardown.mp4 – This is a .png image file which depicts a minor female, approximately 4-5 years old, with her legs spread open, laying on a bed nude except a blue piece of cloth across her stomach. She is being penetrated by an adult male penis.
- File: KS-650M mini video recorder review and teardown.mp4 – This is a .png image file which depicts a nude minor female, approximately 5-6 years old, being subjected

to mouth to penis contact by an adult male.

37. Forensic review also showed that KOESTER's desktop computer was used to access Website A with user ID "reidick" and password "niggerfaggot".

38. During the execution of the aforementioned search warrant, KOESTER voluntarily agreed to be interviewed by law enforcement. During the interview, KOESTER admitted that he owned and maintained several computers at his apartment to include the desktop personal computer found on the desk in his bedroom that contained the 1318 image and 21 video files depicting child sexual abuse material. KOESTER also told law enforcement he has resided at the apartment for approximately the last six or seven months with his roommate.

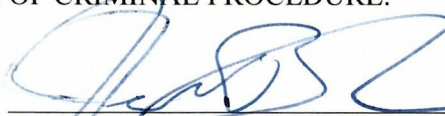
39. KOESTER'S roommate was interviewed by law enforcement during the execution of the aforementioned search warrant as well. KOESTER's roommate stated that the desktop computer in the residence was built and primarily used by KOESTER. The roommate indicated that they had observed KOESTER using the desktop computer primarily for gaming but that they had also observed KOESTER accessing different forums on the computer such as "4chan" and "8chan." The roommate was not familiar with Website A, a username or password starting with "rei" or the Network. Furthermore, the roommate stated that they did not and had not accessed or downloaded or saved any images or videos depicting child sexual abuse material on the desktop computer or any electronic device.

CONCLUSION

41. Based on the foregoing information, there is probable cause to conclude that PHILIP KOESTER has knowingly possessed child pornography that has been transported using any means of interstate and foreign commerce and in and affecting such commerce, in violation of Title 18,

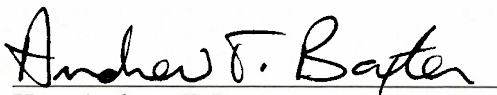
United States Code, Section 2252A(a)(5)(B).

ATTESTED TO BY THE APPLICANT IN ACCORDANCE WITH THE REQUIREMENTS
OF RULE 4.1 OF THE FEDERAL RULES OF CRIMINAL PROCEDURE.



Jenelle Corrine Bringuel
Special Agent
Federal Bureau of Investigation

I, the Honorable Andrew T. Baxter, United States Magistrate Judge, hereby acknowledge that this affidavit was attested by the affiant by telephone on July 1, 2022, in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.



Hon. Andrew T. Baxter
United States Magistrate Judge